NATIONAL SECURITY AGENCY
INFORMATION ASSURANCE DIRECTORATE

Commercial Solutions for Classified (CSfC)
Data-at-Rest (DAR)
Capability Package

Version 1.0
October 15, 2014

CHANGE HISTORY

Title	Version	Date	Change Description
Commercial Solutions for Classified (CSfC) Data-at-rest (DAR) Capability Package	0.8	07/03/2014	Initial draft of CSfC Data-at-Rest (DAR) requirements.
Commercial Solutions for Classified (CSfC) Data-at-rest (DAR) Capability Package	1.0	10/15/2014	Official release of CSfC Data-at-Rest (DAR) requirements.

TABLE OF CONTENTS

1. INTRODUCTION 1
2. PURPOSE OF THIS DOCUMENT 1
3. USE OF THIS DOCUMENT 2
4. DATA-AT-REST PROTECTION OVERVIEW 3
   4.1 SOLUTION STATES 3
   4.2 RATIONALE FOR LAYERED ENCRYPTION 4
   4.3 DAR SUITE B ALGORITHMS 4
   4.4 POSITIVE CONTROL 5
   4.5 RED, GRAY, AND BLACK DATA 6
5. SOLUTION COMPONENTS 6
   5.1 SOFTWARE FULL DISK ENCRYPTION 6
   5.2 FILE ENCRYPTION 7
   5.3 END USER DEVICE 9
      5.3.1 PROVISIONING 9
6. SOLUTION DESIGN 9
   6.1 SWFDE/FE (SF) SOLUTION DESIGN 9
7. THREATS 10
   7.1 PASSIVE THREATS 10
   7.2 EXTERNAL (ACTIVE) THREATS 11
      7.2.1 MALWARE AND UNTRUSTED UPDATES 11
      7.2.2 SOCIAL ENGINEERING 11
   7.3 INSIDER THREATS 11
   7.4 SUPPLY CHAIN THREATS 12
   7.5 INTEGRATOR THREATS 13
8. DAR CONFIGURATION REQUIREMENTS 13
   8.1 REQUIREMENTS DESIGNATORS 14
9. REQUIREMENTS FOR SELECTING COMPONENTS 15
10. CONFIGURATION 16
   10.1 OVERALL SOLUTION REQUIREMENTS 16
   10.2 CONFIGURATION REQUIREMENTS FOR ALL DAR COMPONENTS 17
   10.3 REQUIREMENTS FOR SWFDE COMPONENTS 17
   10.4 REQUIREMENTS FOR FE COMPONENTS 18
   10.5 REQUIREMENTS FOR END USER DEVICES 18
   10.6 CONFIGURATION CHANGE DETECTION REQUIREMENT 20

10.7 REQUIREMENTS FOR DEVICE MANAGEMENT 20
10.8 AUDITING REQUIREMENTS 21
10.9 KEY MANAGEMENT REQUIREMENTS 21
11. REQUIREMENTS SOLUTION OPERATION, MAINTENANCE, & HANDLING ... 22
11.1 REQUIREMENTS FOR THE USE AND HANDLING SOLUTIONS 22
11.2 REQUIREMENTS FOR INCIDENT REPORTING 23
12. ROLE-BASED PERSONNEL REQUIREMENTS 25
13. INFORMATION TO SUPPORT AUTHORIZED OFFICIAL/DESIGNATED APPROVING AUTHORITY 26
13.1 SOLUTION TESTING 26
13.2 RISK ASSESSMENT 27
13.3 REGISTRATION OF SOLUTIONS 28
14. TESTING REQUIREMENTS 28
14.1 PRODUCTION SELECTION 28
14.2 END USER DEVICE CONFIGURATIONS 29
14.3 DAR COMPONENT CONFIGURATION 31
14.4 CONFIGURATION CHANGE DETECTION 33
14.5 AUDIT 33
14.6 KEY MANAGEMENT 34
14.7 IMPLEMENTATION OF GUIDANCE 35
14.8 INCIDENT REPORTING GUIDANCE 35
APPENDIX A. GLOSSARY OF TERMS 36
APPENDIX B. ACRONYMS 39
APPENDIX C. CSFC INCIDENT REPORTING TEMPLATE 42
APPENDIX D. MAPPINGS TO NIST SP 800-53 CONTROLS 43
APPENDIX E. PASSWORD/PASSPHRASE STRENGTH PARAMETERS 47
APPENDIX F. REFERENCES 50

TABLE OF FIGURES

Figure 1: Software Full Disk Encryption 7
Figure 2: Software File Encryption 7
Figure 3: SF Solution Design 10

LIST OF TABLES

Table 1: Approved Suite B DAR Algorithms 4
Table 2: Solution Design Summary 9
Table 3: Requirement Digraphs 14
Table 4: Product Selection Requirements 15
Table 5: Overall Solution Requirements 16
Table 6: Configuration Requirements for All DAR Components 17
Table 7: Requirements for SWFDE Components 17
Table 8: Requirements for FE Components 18
Table 9: Requirements for End User Devices 18
Table 10: Configuration Change Detection Requirements 20
Table 11: Requirements for Device Management 20
Table 12: Auditing Requirements 21
Table 13: Key Management Requirements for All DAR Components 21
Table 14: Requirements for the Use and Handling of Solutions 22
Table 15: Incident Reporting Requirements 24
Table 16: Test Requirements 27
Table 17: Mappings to NIST SP 800-53 Security Controls 43
Table 18: Randomly Generated Minimum Password Length 48
Table 19: Randomly Generated Minimum Passphrase Length 49

1. INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages (CPs) to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CP is vendor-agnostic and provides high-level security and configuration guidance for customers and/or Solution Integrators.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customer and their integrators are advised that modifying a National Information Assurance Partnership (NIAP)-validated component in a CSfC solution may invalidate its certification and trigger a revalidation process. To avoid delays, customers or integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/schedme-pub-6.pdf) to determine whether such a modification will affect the component's certification. In case of a modification to a component, NSA's CSfC Program Management Office will require a statement from NIAP that the modification does not alter the certification, or the security, of the component. Modifications which will trigger the revalidation process include, but are not limited to: configuring the component in a manner different than its NIAP-validated configuration; modifying the original equipment manufacturers' (OEM's) code (to include digitally signing the code).

IAD is delivering a generic CSfC Data-at-Rest (DAR) CP to meet the demand for data-at-rest solutions using a secure sharing suite (S3) of algorithms. These algorithms are used to protect classified data using layers of COTS products. DAR CP Version 1.0 enables customers to implement two independent layers of encryption for the purpose of providing protection for stored information while the End User Device (EUD), defined in Section 5.3, is powered off or in an unauthorized state. This CP takes lessons learned from one proof-of-concept demonstration per solution design that has implemented a set of S3 algorithms, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

2. PURPOSE OF THIS DOCUMENT

This CP provides high-level reference designs and corresponding configuration information allowing customers to select COTS products from the CSfC Components List, available on the CSfC web page (http://www.nsa.gov/ia/programs/csfc_program) for their DAR solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while at rest. As described in Section 9, customers must ensure the components selected from the CSfC Components List will permit the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold requirements,

or the corresponding Objective requirements, applicable to the selected capabilities must be implemented, as described in Section 0. Customers who want to use the solution detailed in this CP must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

3. USE OF THIS DOCUMENT

This document, the CSfC DAR Capability Package Version 1.0, dated September 23, 2014, has been approved by the IAD Director and will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required. Solutions designed according to this Capability Package must be registered with NSA/IAD. Once registered, a signed IAD Registration Acknowledgement will be sent validating that the DAR solution is registered as a CSfC solution to meet the requirements of the latest DAR Capability Package and is approved to protect classified information. Any solution designed according to this Capability Package may be used for one year and must then be revalidated and re-registered by the customer against the most recently published version of the Capability Package.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the DAR Capability Package maintenance team at CSFC_DAR_team@nsa.gov. DAR CP solutions shall comply with National Security Systems (NSS) policy and any conflicts between NSS policy and this CP should be provided to the DAR CP Maintenance team.

The following Legal Disclaimer relates to the use of this CP:

This CP is provided “as is.” Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this CP, even if advised of the possibility of such damage.

The User of this CP agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney’s fees, court costs, and expenses, arising in direct consequence of recipient’s use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4. DATA-AT-REST PROTECTION OVERVIEW

The goal for the DAR solution is to protect classified data when the EUD is powered off or unauthorized. Unauthorized, in this case, means prior to a user presenting and having their credentials (e.g., password, tokens, etc.) validated by both layers of the DAR solution. Specific data to be protected must be determined by the data owner.

4.1 SOLUTION STATES

Powered Off State:

In a powered off state, the device is completely off and not in any power saving state. The EUD is considered unclassified but must still be handled in accordance with the implementing organizations Authorized Official/Designated Approving Authority (AO/DAA) policies.

Powered On and Unauthorized State:

In a powered on and unauthorized state, the EUD is completely on, but the user has not logged in to either layer. The EUD is considered unclassified, but must be handled in accordance with the implementing organization's AO/DAA policies.

Powered On with Outer Layer Authorized State:

In a powered on state with outer layer authorized, the device is operational where the user has authorized to the outer layer of encryption. The device is considered classified and should be handled accordingly.

Powered On with Outer and Inner Layer Authorized State:

In a powered on state with outer and inner layers authorized, the EUD is operational, where the user has authorized to two layers of DAR encryption. The device is considered classified and should be handled accordingly.

Locked State:

In a locked state, the device is powered on but most of the functionality is unavailable for use. User authorization is required to access functionality. This functions as an access control and may provide one layer of DAR protection. The device is considered classified and should be handled accordingly.

4.2 RATIONALE FOR LAYERED ENCRYPTION

A single layer of Suite B encryption, properly implemented, is sufficient to protect classified data-at-rest. The DAR solution uses two layers of Suite B encryption not because of a deficiency in the cryptographic algorithms, but rather to mitigate the risk that a failure in one of the DAR components, whether by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability that results in the exposure of classified information. The use of multiple layers, implemented with components meeting the CSfC vendor diversity requirements reduces the likelihood a single vulnerability can be exploited to reveal protected information.

If one of the DAR layers is compromised or fails in some way, the second DAR layer can still provide the needed encryption to safeguard the classified data. If both layers are compromised or fail simultaneously, it is possible the classified data will become readable to a threat actor. The security of the DAR solution depends on preventing this failure mode by implementing and configuring two independent encryption layers. The goal is to provide redundant protection configured to prevent both layers failing at the same time or that requires an adversary to defeat both mechanisms.

4.3 DAR SUITE B ALGORITHMS

As the portability of EUDs increases, the requirements for when and how classified data is protected also increases. EUDs can be used in both physically protected and physically unprotected environments. Solutions using commercial products must protect classified data on the EUD by using two layers of encryption with approved Suite B algorithms listed in Table 1. The solution design presented in this CP (and future versions of the CP) has specific requirements for configuration, product selection, components, provisioning, authentication, key management, operations, administration, roles, use and handling.

Table 1: Approved Suite B DAR Algorithms

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
Overall Level of Security	128 bits	192 bits	
Confidentiality (Encryption)	AES-128	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature)	ECDSA over the curve P-256 with SHA-256	ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-3 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
	RSA 2048 (prior to 1	N/A	FIPS PUB 186-3

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
	October 2015)		
	DSA 2048 (prior to 1 October 2015)	N/A	FIPS PUB 186-3
Integrity (Hashing)	SHA-256	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Can protect	Up to Secret	Up to Top Secret	

The DAR CP is focused on the implementation of cryptography to mitigate the risk to classified data from unauthorized access when the device is powered off or unauthorized. This CP does not protect against the possibility of malicious code exploits, updates, Operating System (OS) misconfigurations, or the persistence of remnants of key or plaintext material in volatile memory on the EUD when powered on as these are outside of the scope for version 1 of this CP due to a lack of validation support in current protection profiles.

4.4 POSITIVE CONTROL

Although the DAR solution designs can protect the confidentiality of data and render the EUD unclassified, it does not protect the integrity of an EUD outside of the control of approved users. It is difficult to examine and determine whether or not a device has been tampered with. Therefore, the NSA requires implementing organizations to define the circumstances in which an EUD that is part of the organization's solution to be considered outside of the positive control of authorized users (i.e., "lost"). Authorizing Officials (AO) will define the circumstances for considering a device “lost” that aligns with the intended mission and threat environment for which the solution will be deployed. Organizations must also define the circumstances in which an EUD that is a part of that organization's solution is to be considered recovered back into the positive control of authorized users (i.e., "found").

This CP requires any lost device, once found, to be forensically investigated and/or destroyed in order to mitigate threats to the integrity of the EUD and any connected systems, because once found, the device is considered compromised. This requirement to destroy "found" EUDs does not preclude an implementing organization from first performing a forensic examination on a "found" device to discover better ways to protect the organization's EUDs. Authorizing Officials should reference the DAR CP Risk Assessment to help make an informed risk decision.

4.5 RED, GRAY, AND BLACK DATA

This CP uses the following terminology to describe the data types that comprise a DAR solution. The terms Red, Gray, and Black identify the number of encryption layers applied to classified data for a specific EUD state.

Red data is unencrypted classified data being processed by the EUD. After a user successfully authorizes to the outer and inner layers of DAR encryption, the EUD is in a state of processing Red data.

Gray data contains classified information that has been encrypted once. After a user successfully authorizes to the outer layer of DAR encryption, but has not yet authorized to the inner layer of encryption, the EUD is in a state of processing Gray data.

Black data contains classified information that has been encrypted twice. An EUD is considered black when the device is powered off and/or unauthorized and the stored data is encrypted with both the outer and inner layers of DAR encryption.

5. SOLUTION COMPONENTS

5.1 SOFTWARE FULL DISK ENCRYPTION

Software Full Disk Encryption (SWFDE) shown in Figure 1 below is used to provide the outer layer of DAR protection. As defined by National Institute of Standards and Technology (NIST): "Full Disk Encryption (FDE), also known as whole disk encryption, is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authorization to the FDE product." A user must log in to the Pre-Boot Environment (PBE) with valid credentials. Once the user is authorized to the PBE, the SWFDE unencrypts the OS, which allows the computer to boot.

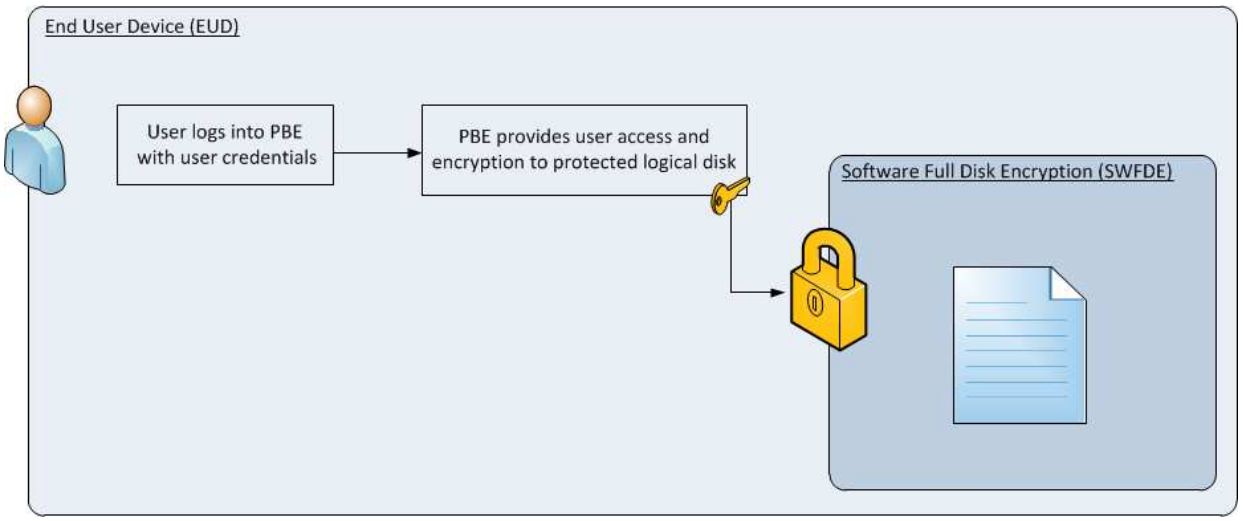

Figure 1: Software Full Disk Encryption

5.2 FILE ENCRYPTION

File Encryption (FE) shown in Figure 2 below is approved to provide the inner layer of DAR protection. File encryption is the process of encrypting individual files or sets of files on an end user devices and permitting access to the encrypted data only after proper authorization is provided.

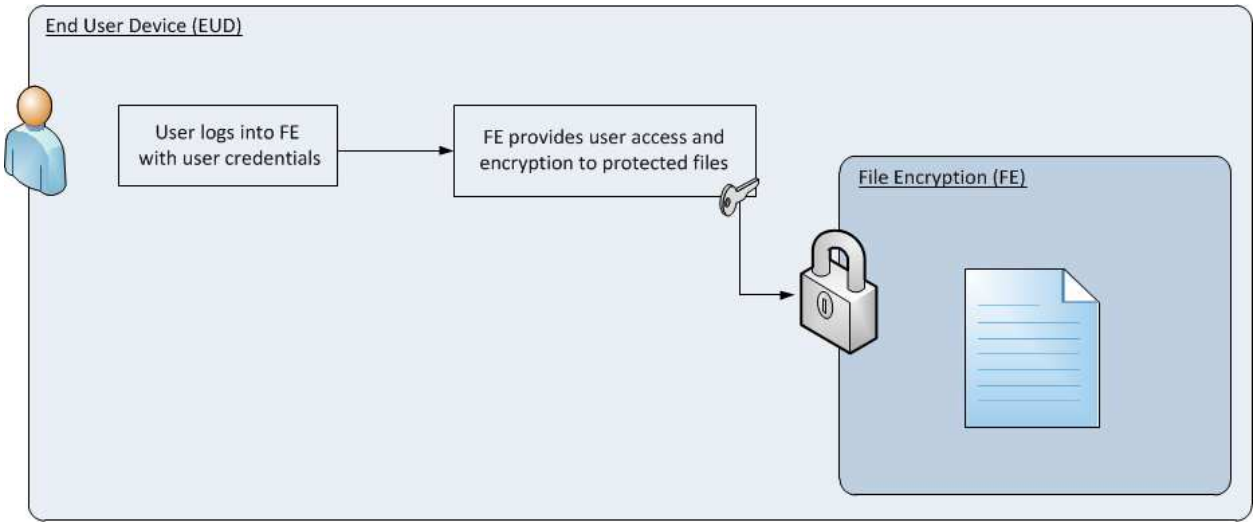

Figure 2: Software File Encryption

File encryption products currently on the market have a wide range of implementations. It is important for the user and implementer to understand how a specific file encryption product operates to ensure they encrypt all classified data on the EUD. There are many events and

applications that may write data to the disk. Users should be made aware of these unless the FE product can encrypt the data without their intervention. Some examples of such events are:

1. Applications permitted to run on the EUD should be carefully considered. Applications may create files (e.g., temporary files) in unprotected locations leaving classified data at risk.
2. Paging files (e.g., swap files) are created when the system runs out of or becomes low on unused volatile memory Random Access Memory (RAM). When this occurs, the system may write to the non-volatile memory (e.g., hard disk) for storage. If the product cannot automatically protect this data, the solution should disable system page files.
3. System restore and other features that allow data to be restored to a previous point in time create copies of the data. If this is enabled it may allow an encrypted file to be restored to a state before it was encrypted. Unless the product accounts for these types of scenarios, these features should be disabled.
4. Memory dump files may be created when an error occurs. Memory dump files may include classified data that existed in volatile memory when the crash occurred. Since these files are created during a system crash, it is likely the product will not be able to properly encrypt them. Therefore, it is recommended this feature be used with care by individuals who understand what data will be contained within file or the feature should be disabled.
5. Printer spool files are created when a document is sent to print. These are used to hold documents while they are in queue for printing. If the solution is going to print any classified information these files should be protected.
6. Moving or deleting files: Users should be informed that moving (cut/paste) a classified file into a protected area is not sufficient for protecting it. Moving or deleting a file while it is unencrypted may leave file contents on the disk until it is overwritten by the file system. This should apply to all file movement for good practice, even though it would not apply in all cases. All files should be encrypted before being deleted or moved.

FE protects the confidentiality of individual files, folders, or volumes, and may be accomplished in several ways. The encryption may be performed by an application, platform, or the host OS. Each encrypted file, folder or volume will be protected by a File Encryption Key (FEK). The FEK is protected by the user's authorization factor, either directly or through one or more Key Encryption Keys (KEKs).

Proper user authentication is required to decrypt the FEK. The FE product will then transparently decrypt files or folders on an individual basis as they are requested by the user via specific applications. To ensure no classified data is left unprotected, the Authorizing Official (AO)/ Designated Approving Authority (DAA) shall be responsible for providing and enforcing a policy which mandates automation and user compliance to encrypt all classified data.

5.3 END USER DEVICE

The End User Device is a personal computer (desktop or laptop) and/or consumer device (e.g., smart phone). An EUD may operate within a secure physical environment, outside of a secure physical environment, or both inside and outside of a secure physical environment as approved by the AO/DAA.

5.3.1 PROVISIONING

Provisioning is the process through which EUDs are initialized before first use. During the provisioning process, the Security Administrator loads and configures the DAR components for the EUD. Provisioning is inherently an out-of-band process requiring physical access to the EUD.

This CP allows for EUD re-provisioning or reuse of DAR components as long as it is performed in accordance with this CP. If re-provisioning, the unencrypted data secured on the device must be at the same classification level of the previous unencrypted data stored on the approved DAR solution. Re-provisioning EUD components from any other solution design or non-CSfC solution is prohibited.

6. SOLUTION DESIGN

The CP provides the solution design listed in Table 2 below. This design describes a solution meeting a wide variety of requirements to protect classified DAR.

The two-layer design consisting of SWFDE and FE is designated “SF”.

Table 2: Solution Design Summary

Solution Design	Designator	Description
SWFDE / FE	SF	DAR solution design that uses FE as the inner layer and SWFDE as the outer layer, as described in Section 6.1. Typically intended for servers, desktops, some laptops, and some tablets.

The solution is contained in an individual EUD. The implementation must meet all threshold requirements in the appropriate solution design section.

6.1 SWFDE/FE (SF) SOLUTION DESIGN

The SF Solution Design approach requires software full disk encryption and file/folder/volume encryption. In the SF solution design, SWFDE will be used to provide DAR protection for the outer layer and the inner layer will be provided by the FE product. The SF DAR solution uses a password, smart card, or Universal Serial Bus (USB) token to provide access to classified data. Once a user inputs the correct password, smart card, or USB token, the system boots the

operating system. Next, the user authorizes to the FE which in turn decrypts the user's classified file. The SF solution is depicted below in Figure 3.

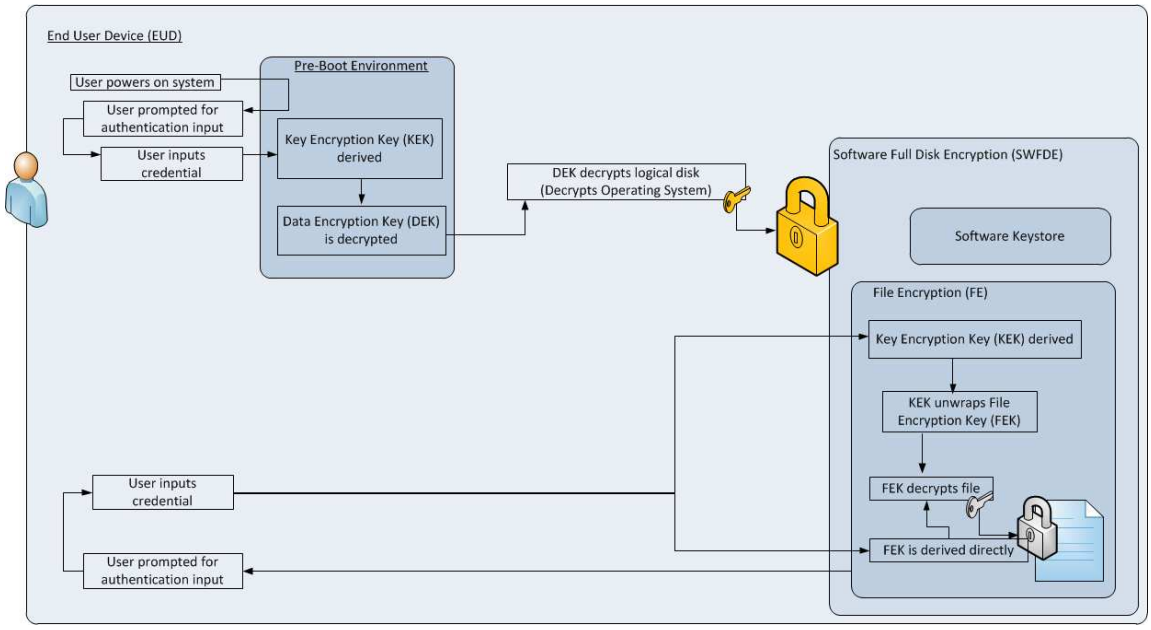

Figure 3: SF Solution Design

Each layer of encryption in the SF DAR solution may use similar authorization mechanism types (e.g., passwords, tokens) but requires a unique authorization credential for each layer. For the first layer of encryption the user will authorize to the Pre-Boot Environment (PBE) provided by the SWFDE. For the second layer the user will use their OS login credentials, application credentials, or file-specific credentials to authorize to the FE.

7. THREATS

This section details how the required components work together to provide overall security in the solution. Figure 3 shows the boundary of the DAR solution covered by this CP. An assessment of security was conducted on the design described in this CP while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of protecting data-at-rest. By examining these threats the organization will have a better understanding of the risk they are accepting and how these risks affect the Confidentiality, Integrity, and Availability of the data.

7.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the EUD without changing the state of the system.

The security against passive attack targeting the DAR on the EUD is provided by the layered encryption. To mitigate passive attacks, two layers of Suite B encryption are employed to provide confidentiality for the solution. Use of Advanced Encryption Standard (AES) is approved to protect classified information, meeting IAD and Committee on National Security Systems Policy (CNSSP) - 15 guidance for adequate confidentiality. The DAR components used to set up the layers of encryption must be independent in a number of ways (see Section 8). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both layers of encryption.

7.2 EXTERNAL (ACTIVE) THREATS

This threat refers to outsiders gaining unauthorized access to classified Red data on the EUD. Threat actions include brute force attacks, or introduction of malware with the intention to compromise the EUD and gain access to Red data. Adversaries could gain access to the EUD and then exploit other devices once the EUD is connected to a network.

One method for preventing unauthorized access from an external attack is a reasonable password policy. It is required that each encryption layer have a form of user authentication. This will ensure that the data residing on the EUD will still be protected with at least one layer of encryption if the adversary is able to access one of the layers in the solution.

7.2.1 MALWARE AND UNTRUSTED UPDATES

Each DAR component of this solution has the option to receive updates only through direct physical administration or an NSA approved Data-in-Transit (DIT) solution. This mitigates the threats of malicious users trying to push updates or code patches that can affect the security of the components. The source of all updates and patches shall be verified via digital signature before installation occurs.

7.2.2 SOCIAL ENGINEERING

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against social engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in Section 7.

7.3 INSIDER THREATS

This threat refers to an unauthorized or cleared person or group of people with access, physical or logical, to the EUD who may act maliciously or negligently, resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain unauthorized access to the device, dishonest employees, or those that have the means and desire to gain access to the data residing on the EUD.

Threat actions include insertion or omission of data entries that result in loss of data integrity, willingly changing the configuration of an EUD, unwillingly or unknowingly executing a virus or malware, intentionally exposing the device to a virus or malware, cross-contaminating a EUD with data from a higher classification to a lower classification (e.g., Secret data to unclassified device). Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 12). In addition it is recommended that each user of the solution have a unique user account (see Section 10.1).

7.4 SUPPLY CHAIN THREATS

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the Information and Communication Technology (ICT) components embedded in the systems upon which the ability to perform their mission rely. The supply chain for those ICT components are the underpinnings of those systems and networks and supply chain attacks are attempts to proactively compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component. They are only able to provide assurances based on their reliance of established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify and test, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine the source of where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA-approved Product Supply Chain Threat Assessment process (See CNSSD 505 SCRM for additional guidance).

There are doctrinal requirements placed on Product Selection, Implementers, and Solution Integrators of these solutions to minimize the threat of supply chain attacks (see Sections 8, 10, and 11).

7.5 INTEGRATOR THREATS

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different than a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures. In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the DAR solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution.

More information on the NSA's list of trusted integrators can be found on the NSA CSfC Website in the "Criteria For CSfC Integrators" section (link: https://www.nsa.gov/ia/programs/csfc/index.shtml)

8. DAR CONFIGURATION REQUIREMENTS

Sections 0 through 13 specify requirements for implementations of the SF solution compliant with this CP. The tables of requirements in the following sections specify the solution design each requirement is applicable to:

- SF design: DAR solution components include SWFDE and FE.

The CP includes two categories of requirements specified based on the guidance provided below:

- An Objective (O) requirement specifies a feature or function that is desired or expected. Organizations should implement objective requirements in lieu of a corresponding Threshold requirement where feasible.

- A Threshold (T) requirement specifies a minimum acceptable feature or function that still provides the needed capabilities if the corresponding objective requirement cannot

reasonably be met (e.g., due to system maturity). A solution implementation must satisfy all applicable Threshold requirements, or their corresponding Objective requirements, in order to comply with this CP.

In many cases, the Threshold requirement also serves as the Objective requirement (T=O). In some cases, multiple versions of a requirement may exist in this Capability Package. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement. Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement improves upon the Threshold requirement and may replace the Threshold requirement in future versions of this CP. Objective requirements without a corresponding Threshold requirement are marked as "Optional", but improve upon the overall security of the solution and should be implemented where feasible.

In order to comply with this CP, a solution must at minimum implement all Threshold requirements associated with each of the solution designs it supports, and should implement the Objective requirements associated with those solution designs where feasible. For example, a DAR solution utilizing a SWFDE and FE must implement the Threshold requirements only applicable to the SF design.

8.1 REQUIREMENTS DESIGNATORS

Each requirement defined in this CP has a unique identifier digraph that groups related requirements together (e.g., KM), and a sequence number (e.g., 2). Table 3 below lists the digraphs used to group together related requirements, and identifies where they can be found in the following sections.

Table 3: Requirement Digraphs

Digraph	Description	Section(s)	Table(s)
PS	Product Selection Requirements	Section 9	Table 4
SR	Overall Solution Requirements	Section 10.1	Table 5
CR	Configuration Requirements for All DAR Components	Section 10.2	Table 6
SW	Requirements for SWFDE Components	Section 10.3	Table 7
FE	Requirements for FE Components	Section 10.4	Table 8
EU	Requirements for EUD	Section 10.5	Table 9
CM	Configuration Change Detection Requirements	Section 10.6	Table 10
DM	Requirements for Device Management	Section 10.7	Table 11
AU	Auditing Requirements	Section 10.8	Table 12
KM	Key Management Requirements for All DAR Components	Section 10.9	Table 13

Digraph	Description	Section(s)	Table(s)
GD	Requirements for Use and Handling of Solutions	Section 11.1	Table 14
RP	Requirements for Incident Reporting	Section 11.2	Table 15
TR	Testing Requirements	Section 13.1	Table 16

9. REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 4: Product Selection Requirements

Req #	Requirement Description	Solution Designs	Threshold/Objective	Alternative
DAR-PS-1	The products used for the FE layer shall be chosen from the list of FE products on the CSfC Components List.	SF	T=O	
DAR-PS-2	The products used for the SWFDE layer shall be chosen from the list of SWFDEs on the CSfC Components List.	SF	T=O	
DAR-PS-3	The Inner and Outer DAR layer shall either: • Come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • Be different products from the same manufacturer, where NSA has determined that the products meet the CSfC Program's criteria for implementation independence.	SF	T=O	

Req #	Requirement Description	Solution Designs	Threshold/Objective	Alternative
DAR-PS-4	Each component selected from the CSfC Components List shall go through a Product Supply Chain Risk Management Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA approved Product Supply Chain Threat Assessment process. (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance.)	SF	T=O	
DAR-PS-5	The cryptographic libraries used by the Inner and Outer DAR layer shall be independently developed and implemented.	SF	O	optional

10. CONFIGURATION

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components for a DAR solution.

10.1 OVERALL SOLUTION REQUIREMENTS

Table 5: Overall Solution Requirements

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-SR-1	Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed.	SF	T=O	
DAR-SR-2	The DAR solution shall be properly configured according to local policy and U.S. Government guidance (e.g., NSA guidelines). In the event of conflict between the requirements in this CP and local policy, the CSfC Program Management Office (PMO) must be contacted.	SF	T=O	
DAR-SR-3	Each DAR component shall have unique user accounts.	SF	O	optional

10.2 CONFIGURATION REQUIREMENTS FOR ALL DAR COMPONENTS

Table 6: Configuration Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-CR-1	Default encryption keys shall be changed.	SF	T=O	
DAR-CR-2	User authentication credential values for each DAR layer mechanism type shall be unique (e.g., the password for the SWFDE will not be the same as the password for the FE)	SF	T=O	
DAR-CR-3	DAR components shall use algorithms for encryption selected from Table 1 that are approved to protect the highest classification level of the data.	SF	T=O	
DAR-CR-4	Each DAR component shall prevent further authorization attempts after a number of failed attempts defined by the AO/DAA.	SF	O	optional
DAR-CR-5	Each DAR layer shall zeroize the DEK/FEK after a number of consecutive failed logon attempts defined by the AO/DAA.	SF	O	optional
DAR-CR-6	Each DAR component shall locally generate its own symmetric encryption keys on the EUD.	SF	T=O	
DAR-CR-7	Each DAR component shall permit only an administrator to disable DAR component.	SF	O	optional
DAR-CR-8	All components shall have DAR protections enabled at all times after provisioning.	SF	T=O	
DAR-CR-9	All components shall encrypt all classified data.	SF	T=O	
DAR-CR-10	All CSfC components shall be implemented (configured) using only their National Information Assurance Partnership (NIAP)-approved configuration settings.	SF	T=O	
DAR-CR-11	Users shall be restricted to designated user folders.	SF	T=O	

10.3 REQUIREMENTS FOR SWFDE COMPONENTS

Table 7: Requirements for SWFDE Components

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-SW-1	The SWFDE shall use Cipher Block Chaining (CBC) for encryption.	SF	T	DAR-SW-2
DAR-SW-2	The SWFDE shall use (XTS) for encryption.	SF	O	DAR-SW-1

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-SW-3	The SWFDE shall be configured to use one of the following authentication options: • A randomly generated passphrase or password that meets the minimum strength set in APPENDIX E. Password/Passphrase Strength Parameters or • A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or • A combination of both of the above.	SF	T=O	

10.4 REQUIREMENTS FOR FE COMPONENTS

Table 8: Requirements for FE Components

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-FE-1	The FE shall use CBC or XTS for Encryption.	SF	T=O	
DAR-FE-2	The FE shall use one of the following authentication options: • A randomly generated or user generated passphrase or password defined by the AO/DAA that meets minimum strength set in APPENDIX E. Password/Passphrase Strength Parameters; or • An external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1.	SF	T=O	

10.5 REQUIREMENTS FOR END USER DEVICES

Table 9: Requirements for End User Devices

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-EU-1	All EUD provisioning shall be performed through direct physical access.	SF	T=O	
DAR-EU-2	The EUD's non-volatile storage media shall be destroyed per National Telecommunication and Information Systems Security Instruction 4004 if found after being lost. (This does not preclude forensic investigation by appropriate authority.)	SF	T=O	
DAR-EU-3	EUDs shall implement the Basic Input/Output System (BIOS) security guidelines specified in NIST SP 800-147.	SF	O	optional

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-EU-4	All Users shall sign an organization-defined user agreement before being authorized to use an EUD.	SF	T=O	
DAR-EU-5	All Users shall receive an organization-developed training course for operating an EUD prior to use.	SF	T=O	
DAR-EU-6	At a minimum, the organization defined user agreement shall include each of the following: • Operational Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when and where the EUD may be used • Verification of Information Assurance (IA) Training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities • An overview of what constitutes positive control and the risks associated with using the EUD after it is lost	SF	T=O	
DAR-EU-7	External USB tokens and Smartcards, when used, shall be removed from the EUD upon or before shut down in accordance with AO/DAA policy.	SF	T=O	
DAR-EU-8	AO/DAA shall provide guidance on storing and securing authentication factors.	SF	T=O	
DAR-EU-9	The Security Administrator shall disable system power saving states on EUDs (i.e., Sleep and Hibernate).	SF	T=O	
DAR-EU-10	The EUD shall power off after a period of inactivity defined by the AO/DAA.	SF	T=O	
DAR-EU-11	The EUDs shall be provisioned within a physical environment certified to protect the highest classification level of the data stored on the device.	SF	T=O	
DAR-EU-12	The EUD shall only be re-provisioned to the same or higher classification level of the classified data per an AO/DAA approved process.	SF	T=O	
DAR-EU-13	The EUD shall be reported as “lost” when out of positive control as specified by the AO/DAA.	SF	T=O	
DAR-EU-14	System folders shall have user write permissions disabled unless authorized by an administrator.	SF	T=O	

10.6 CONFIGURATION CHANGE DETECTION REQUIREMENT

Table 10: Configuration Change Detection Requirements

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-CM-1	A history of baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor.	SF	T=O	
DAR-CM-2	An automated process shall ensure configuration changes are logged.	SF	O	optional
DAR-CM-3	Log messages generated for configuration changes shall include the specific changes made to the configuration.	SF	O	optional

10.7 REQUIREMENTS FOR DEVICE MANAGEMENT

Only authorized Security Administrators (See Section 12) will be allowed to administer the DAR Components.

Remote administration for software updates and re-configuration can be utilized through an approved NSA DIT solution.

If the solution owner is unable to remotely manage the EUDs, the solution owner must physically manage all devices in order to ensure the device(s) and DAR protection components receive the proper software and configuration updates.

Table 11: Requirements for Device Management

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-DM-1	EUDs shall be physically administered.	SF	T	
DAR-DM-2	EUDs shall be remotely administered using a NSA approved DIT protection solution (e.g., NSA Certified Product or CSfC approved solution).	SF	O	DAR-DM-1
DAR-DM-3	Administration Workstations shall be dedicated for the purposes given in the Capability Package and shall be physically separated from workstations used to manage non-CSfC solutions.	SF	T=O	
DAR-DM-4	Administration Workstations shall physically reside within a protected facility where CSfC solution(s) are managed.	SF	T=O	

10.8 AUDITING REQUIREMENTS

Table 12: Auditing Requirements

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-AU-1	EUDs shall be inspected for malicious physical changes in accordance with AO/DAA defined policy.	SF	T=O	
DAR-AU-2	The EUDs shall be configured to generate an audit record of the following events: • Start-up and shutdown of any platform audit functions. • All administrative actions affecting the DAR encryption components. • User authorization attempts and success/failure of the attempts. • Software updates to the DAR encryption components.	SF	O	optional
DAR-AU-3	Auditors shall review audit logs for an AO/DAA defined time period.	SF	T=O	
DAR-AU-4	Auditors shall physically account for the EUDs after an AO/DAA defined time period.	SF	T=O	
DAR-AU-5	Administrators shall periodically compare solution component configurations to a trusted baseline configuration after an AO/DAA defined time period.	SF	O	optional

10.9 KEY MANAGEMENT REQUIREMENTS

Table 13: Key Management Requirements for All DAR Components

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-KM-1	The KEK, FEK, and DEK key sizes and algorithms used for the SWFDE and FE shall be as specified in Table 1.	SF	T=O	
DAR-KM-2	DAR solution products shall be initially keyed within a physical environment certified to protect the highest classification level of the DAR solution.	SF	T=O	
DAR-KM-3	The DAR solution shall disable all key recovery mechanisms.	SF	T=O	

11. REQUIREMENTS SOLUTION OPERATION, MAINTENANCE, & HANDLING

11.1 REQUIREMENTS FOR THE USE AND HANDLING SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

Table 14: Requirements for the Use and Handling of Solutions

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-GD-1	Acquisition and procurement documentation shall not include information about how the equipment will be used, including that it will be used to protect classified information.	SF	T=O	
DAR-GD-2	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the Capability Package.	SF	T=O	
DAR-GD-3	The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the DAR Capability Package.	SF	T=O	
DAR-GD-4	Results of the compliance audit shall be provided to and reviewed by the AO/DAA.	SF	T=O	
DAR-GD-5	When a new approved version of the DAR Capability Package is published by NSA, the AO/DAA shall ensure compliance against this new Capability Package within 6 months.	SF	T=O	
DAR-GD-6	Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or less) months (see Section 13.3).	SF	T=O	
DAR-GD-7	The Security Administrator, Auditor, User, and all Solution Integrators shall be cleared to the highest level of data protected by the DAR solution.	SF	T=O	
DAR-GD-8	The Security Administrator and Auditor roles shall be performed by different people.	SF	T=O	
DAR-GD-9	All Security Administrators, Users, and Auditors shall meet local information assurance training requirements.	SF	T=O	
DAR-GD-10	User shall report lost or stolen EUDs to their Information System Security Officer (ISSO) or chain of command as defined by the AO/DAA.	SF	T=O	

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-GD-11	Only Security administrators shall perform the installation and policy configuration.	SF	T=O	
DAR-GD-12	Security critical patches (such as Information Assurance Vulnerability Alert (IAVAs) shall be tested and subsequently applied to all components in the solution in accordance with local policy and this Capability Package.	SF	T=O	
DAR-GD-13	Local policy shall dictate how the Security Administrator will install patches to solution components.	SF	T=O	
DAR-GD-14	All DAR components shall be updated using digitally signed updates provided by the vendor.	SF	T=O	
DAR-GD-15	All authorized Users shall have the ability to zeroize keys for both layers.	SF	O	optional
DAR-GD-16	When using an FE Product, the user must ensure that no classified data shall be put into the file's metadata (e.g., filename)	SF	T=O	
DAR-GD-17	All components in the solution shall be disposed of as classified devices, unless declassified using AO/DAA-approved procedures.	SF	T=O	
DAR-GD-18	Users shall identify and select all classified data that must be encrypted.	SF	T=O	
DAR-GD-19	AO/DAA shall define loss of positive control for each use case.	SF	T=O	

11.2 Requirements for Incident Reporting

Table 15 lists requirements for reporting security incidents to NSA that are to be followed in the event a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators (SAs) and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for Operations and Maintenance (O&M) will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Compromise, in this context, includes reporting real or perceived access to classified data (e.g., user or administrator access or permission to data without having to authorize or using incorrect credentials).

Table 15 only provides requirements directly related to the incident reporting process. See Section 10.8 for requirements supporting detection of events that may reveal that a reportable incident has occurred.

Table 15: Incident Reporting Requirements

Req #	Requirement Description	Solution Designs	Threshold/ Objective	Alternative
DAR-RP-1	Report a security failure in any of the CSfC DAR solution components.	SF	T=O	
DAR-RP-2	Report any malicious configuration changes to the DAR components	SF	T=O	
DAR-RP-3	Report any evidence of a compromise of classified data caused by a failure of the CSfC DAR solution.	SF	T=O	
DAR-RP-4	Report any evidence of malicious physical tampering (e.g., missing or mis-installed parts) with solution components.	SF	T=O	
DAR-RP-5	Confirmed incidents meeting the criteria in DAR-RP-1 through DAR-RP-4 shall be reported within 24 hours of detection via Joint Incident Management System (JIMS) or contacting the NSA as specified in the CSfC Registration Letter.	SF	T=O	
DAR-RP-6	At a minimum, the organization shall provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No)	SF	T=O	

12. ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are detailed below, along with doctrinal requirements for these roles.

End User – An End User may operate a EUD from physical locations not owned, operated, or controlled by the government. The End User shall be responsible for operating the EUD in accordance with this CP and an organization defined user agreement. End User duties include, but are not limited to:

1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.
2) Alerting the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

Security Administrator – The Security Administrator shall be responsible for maintaining monitoring, and controlling all security functions for the entire suite of products composing the DAR solution. Security Administrator duties include but are not limited to:

1) Ensuring that the latest security critical software patches and updates (such as IAVAs) are applied to each product in a timely fashion.
2) Documenting and reporting security-related incidents to the appropriate authorities.
3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic supports activities may require that the Security Administrator escort uncleared personnel.
4) Ensuring that the implemented DAR solution remains compliant with the latest version of the CP.
5) Provisioning and maintaining EUDs in accordance with this CP.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and events recorded in the audit logs to ensure that no action or event represents a compromise of the DAR solution. The role of Auditor and Security Administrator shall not be performed by the same individual. Auditor duties include but are not limited to:

1) Reviewing, managing, controlling, and maintaining security audit log data
2) Documenting and reporting security related incidents to the appropriate authorities.
3) The Auditor will only be given authority to access all audit record.

Solution Integrator – In certain cases, an external integrator may be hired to implement a DAR solution based on the CP. Solution Integrator duties may include but are not limited to:

1) Acquiring the products that compose the solution.
2) Configuring the DAR solution in accordance with the CP.
3) Testing the DAR solution.
4) Documenting the solution and its compliance to the CP.
5) Troubleshooting the solution.

13. INFORMATION TO SUPPORT AUTHORIZED OFFICIAL/DESIGNATED APPROVING AUTHORITY

This section details items that likely will be necessary for the customer to obtain approval from the system AO/DAA. The customer and AO/DAA have obligations to perform the following:

- The customer, possibly with support from a Solution Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a Test Plan and perform testing of the DAR solution, see Section 13.1.
- The customer has system assessment and authorization performed using the risk assessment information referenced in Section 13.2.
- The customer provides the results from testing and system assessment and authorization to the AO/DAA for use in making an approval decision. The AO/DAA is ultimately responsible for ensuring that all requirements from the CP have been properly implemented. NSA publishes compliance matrixes requiring a short description of how requirements are met. NSA recommends the AO/DAA require the compliance matrix as part of their body of evidence.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 13.3. NSA publishes registration forms on NSA.gov.
- Customers who want to use a variant of the solution detailed in this CP will contact NSA early in their design phase to determine ways to obtain NSA approval.
- The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the DAR CP, and the results shall be provided to the AO/DAA.

13.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a DAR solution. This T&E will be a critical part of the approval process for the AO/DAA, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the DAR solution. The entire solution, to include each component described in Section 5, is addressed by this test plan.

1) Set up the baseline network design and configure all components.
2) Document the baseline network design configuration. Include product model and serial numbers, and software version numbers as a minimum.
3) Develop a test plan for the specific implementation using the test objectives from Section 14. Any additional requirements imposed by the local AO/DAA should also be tested, and the test plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.
4) Perform testing using the test plan derived in Step 3. System testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a final test report to be delivered to the AO/DAA for approval of the solution.
6) The following testing requirement has been developed to ensure that the DAR solution functions properly and meets the configuration requirements from Section 8. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 16: Test Requirements

Req #	Requirement Description	Solution Designs	Threshold/ Objective
DAR-TR-1	The organization implementing the CP shall perform all tests listed in Section 14.	SF	T=O

13.2 Risk Assessment

The Risk Assessment (RA) of the DAR solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request the risk assessment, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the RA is available on the SIPRNet CSfC website. The AO/DAA shall be provided a copy of the NSA RA for their consideration in approving the use of the solution.

13.3 REGISTRATION OF SOLUTIONS

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. Customers will provide their compliance checklists and registration forms to NSA. This registration will allow NSA to track where DAR CP solutions are instantiated and to provide AO/DAAs at those sites with appropriate information, including all significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process, as well as the compliance matrices and registration forms, are available at http://www.nsa.gov/ia/programs/csfc_program.

Solution registrations are valid for one year, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this CP that has been approved by the IAD Director is published, customers will have six months to bring their solutions in compliance with the new version and re-register their solution (see requirement DAR-GD-5). Customers are also required to update their registrations whenever the information provided on the registration form changes.

14. TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or Solution Integrator to ensure they have properly configured the solution. As defined in Section 0, in order to comply with this CP, a solution must, at minimum, implement all Threshold requirements associated with each of the capabilities it supports, and should implement the Objective requirements associated with those capabilities where feasible. These tests may also be used to provide evidence to the AO/DAA regarding compliance of the solution within this CP. Note that the details of the procedures are the responsibility of the final developer of the test plan in accordance with AO/DAA-approved network procedures. The AO/DAA is ultimately responsible for ensuring that all requirements from the CP have been properly implemented.

14.1 PRODUCTION SELECTION

This section contains a procedure to verify that the FE and SWFDE were selected to ensure independence in several important features.

Requirements being tested: DAR-PS-1 through DAR-PS-5.

Procedure Description:

1) For each DAR layer, perform the following:

    a) Verify that the FE is on the list of FEs on the CSfC Components List. (DAR-PS-1)

    b) Verify that the SWFDE is on the list of FDEs on the CSfC Components List. (DAR-PS-2)

    c) Verify that that the SWFDE and FE either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (DAR-PS-3 and DAR-PS-5)

    d) Verify that each component selected from the CSfC Components List goes through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA approved Product Supply Chain Threat Assessment process. (See CNSSD 505 SCRM for additional guidance.) (DAR-PS-4)

Expected Results:

The results of the inspection should reveal that the DAR Solution components conform to the DAR CP.

14.2 END USER DEVICE CONFIGURATIONS

This section contains procedures to ensure that the configurations for all the EUDs in the DAR solution follow the requirements in this Capability Package.

Requirements being tested: DAR-EU-1, DAR-EU-3 through DAR-EU-14, DAR-SR-3, and DAR-DM-1 through DAR-DM-2.

Procedure Description:

1) For each EUD perform the following:
    a) Ensure the implementing organization policy states that provisioning the EUD takes place in a facility that is equal to the highest classification level DAR solution and done through direct physical access. (DAR-EU-1 and DAR-EU-11)
    b) Inspect the EUD's BIOS in order to verify that the BIOS comply with the security guidelines found in NIST-SP 800-147. (DAR-EU-3)
    c) Ensure the implementing organization policy states that all users are required to sign an organization-defined user agreement before being authorized to use a EUD. (DAR-EU-4)

d) Verify the implementing organization has a training program in place for users to receive prior to operating a EUD. (DAR-EU-5)
e) Verify that at a minimum, the organization defined user agreement shall include each of the following (DAR-EU-6):
    - Operational Security (OPSEC) guidance
    - Required physical protections to employ when operating and storing the EUD
    - Restrictions for when and where the EUD may be used
    - Verification of Information Assurance (IA) Training
    - Verification of appropriate clearance
    - Justification for Access
    - Requester information and organization
    - Account Expiration Date
    - User Responsibilities
    - An overview of what constitutes positive control and the risks associated with using the EUD after it is lost
f) Ensure all system power states on EUDs are disabled by the Security Administrator (i.e., Sleep and Hibernate). (DAR-EU-9)
g) Ensure the EUD is configured to shut down for after a period of inactivity defined by the AO/DAA. (DAR-EU-10)
h) Ensure the EUD is only re-provisioned to the same or higher classification level of the classified data per an AO/DAA approved process. (DAR-EU-12)
i) Verify that the implementing organization policy states that a EUD is considered and shall be reported as "lost" if out of positive control as specified by the AO/DAA. (DAR-EU-13)
j) Verify that the EUD has unique user accounts for each user. (DAR-SR-3)
k) Ensure that EUDs are physically administered and that procedures are in place to perform this. (DAR-DM-1)
l) Ensure that EUDs are remotely administered using a NSA approved DIT protection solution (e.g. NSA Certified Product or CSfC approved solution). (DAR-DM-2)
m) Ensure Administration Workstations are dedicated and physically separated from workstations used to manage non-CSfC solutions. (DAR-DM-3)
n) Ensure Administration Workstations physically reside within a protected facility where CSfC solution(s) are managed. (DAR-DM-4)

2) If the EUD requires any external authentication factors, perform the following:
    a) Ensure the implementing organization policy states that USB tokens and Smartcards, when used, shall be removed from the EUD upon or before shut down in accordance with AO/DAA policy. (DAR-EU-7)
    b) Ensure that the AO/DAA provides guidance on storing and securing authentication factors. (DAR-EU-8)

Expected Results:

For step 1, all EUDs should be configured properly. For step 2, an EUD utilizing a token should follow organizational policy for handling and storing authentication factors.

14.3 DAR COMPONENT CONFIGURATION

This section contains procedures to ensure that the configurations for all the DAR Components in the DAR solution follow requirements given in this Capability Package.

Requirements being tested: DAR-SR-1, DAR-SR-2, DAR-CR-1 through DAR-CR-11, DAR-EU-14, DAR-SW-1 through DAR-SW-3, DAR-FE-1, DAR-GD-15, DAR-KM-1, and DAR-KM-3.

Procedure Description:

1) For each DAR component in the solution, perform the following:
    a) Obtain the current configuration for the DAR Component
    b) Verify that all default accounts, passwords, community strings, and other default access control mechanisms are changed or removed. (DAR-SR-1)
    c) Verify that the component is configured according to local policy and U.S. Government guidance. (e.g., NSA Guidelines). In the event of conflict between the requirements in this CP and local policy, the CSfC PMO must be contacted. (DAR-SR-2)
    d) Change the authentication passwords to ensure that all default encryption keys are changed before the component is used. (DAR-CR-1)
    e) Verify that the user authentication credentials for each DAR layer mechanism type are unique. (DAR-CR-2)
    f) Ensure that DAR components use algorithms for encryption selected from Table 1, which are approved to protect the highest classification level of the data. (DAR-CR-3)
    g) Enter the number of failed attempts as defined by the AO/DAA to ensure that the user is locked out and is not allowed any further authentication attempts. (DAR-CR-4).

h) Enter the number of wrong passwords consecutively as defined by the AO/DAA and verify that the Data Encryption Key (DEK) is zeroized by each DAR layer. (DAR-CR-5)
i) Ensure each DAR component generates its own symmetric encryption keys. (DAR-CR-6)
j) Ensure that each DAR component is configured to enable only an administrator to disable DAR component. (DAR-CR-7)
k) Ensure that all components have DAR protections enabled at all times after provisioning. (DAR-CR-8)
l) Ensure all components encrypt all selected classified data. (DAR-CR-9)
m) Ensure all CSfC components are implemented (configured) using only their NIAP-approved configuration settings. (DAR-CR-10)
n) Ensure that all key sizes and algorithms used for the DAR components use the algorithms as specified in Table 1. (DAR-KM-1)
o) Verify that all key recovery mechanisms are disabled. (DAR-KM-3)

2) For each SWFDE component in the solution, perform the following:
   a) Verify the SWFDE uses either CBC or XTS for encryption. (DAR-SW-1, DAR-SW-2)
   b) Verify that SWFDE is configured to use one of the following authentication options (DAR-SW-3):
      - A randomly generated passphrase or password that meets the minimum strength set in APPENDIX E. Password/Passphrase Strength Parameters or
      - A randomly-generated bit string equivalent to the cryptovariable strength of the DEK contained on an external USB token or
      - A combination of both of the above.
3) For each FE component in the solution, perform the following:
   a) Verify that user write permissions to system folders are disabled unless authorized by an administrator. (DAR-EU-14)
   b) Verify that only CBC or XTS are utilized for encryption. (DAR-FE-1)
   c) Ensure that the zeroization of all cryptographic keys is enabled per AO/DAA guidelines. (DAR-GD-15)
   d) Verify that each user is restricted to their designated user folder. (DAR-CR-11)
   e) Verify that only the administrator has privileges to disable data-at-rest protection. (DAR-CR-7)
   f) Verify that the FE uses one of the following authentication options (DAR-FE-2):
      - A passphrase or password with the length and complexity defined in APPENDIX E. Password/Passphrase Strength Parameters; or an external

smartcard or software capability containing a software certificate with RSA or ECC key pairs.

Expected Results:

For step 1, verify that the SWFDE DAR component is properly configured and operating correctly. For step 1 and 3, verify that the FE DAR component is properly configured and operating correctly.

14.4 CONFIGURATION CHANGE DETECTION

This section contains procedures to ensure that changes made to any of the DAR Component configurations are detected by the Configuration Change Detection tool.

Requirements being tested: DAR-CM-1 through DAR-CM-3, DAR-AU-5.

Procedure Description:

1) The following steps shall be done for each of the DAR Components within the solution.
   a) Ensure that a baseline configuration for all components is maintained by the Security Administrator and is made available to the Auditor. (DAR-CM-1)
   b) Verify that procedures are in place for Administrators to periodically compare solution component configurations to a trusted baseline configuration after an AO/DAA defined time period. (DAR-AU-5)
   c) Ensure an automated process is enabled to log all configuration changes. (DAR-CM-2)
   d) Make a configuration change. Look in the audit log to verify that a log entry has been generated about the configuration change and that the specific changes are properly recorded. Do this several times with different types of changes, and then return to the initial configuration to complete. (DAR-CM-3)

Expected Results:

The Auditor will validate the baseline configuration was stored in Step 1a. In Step 1d, there should be a log entry created for each configuration change in the audit log including the actual configuration change.

14.5 AUDIT

This section contains procedures for ensuring audit events are detected, the proper information is logged for each event.

Requirements being tested: DAR-AU-1 through DAR-AU-4.

Procedure Description:

1) Verify that EUDs are inspected for malicious physical changes in accordance with AO/DAA defined policy. (DAR-AU-1)

2) Examples for testing the ability of each DAR Component to audit and log audit events specified in the CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry. (DAR-AU-2)

    a) Startup and shutdown the EUD and any platforms therein that operate independently. Review the audit logs to verify that the startup and shutdown events are recorded.

    b) Verify that any actions taken as an administrator affecting the DAR encryption components are logged.

    c) Authorize to both layers on the EUD successfully. Then logout and attempt to re-authorize to both layers but purposely enter the wrong authentication credentials. Review the audit logs to verify the success/failure of authentication attempts.

    d) Send software updates to the DAR encryption components to verify that the updates are recorded in the audit log.

3) Inspect the organization's implementation policy to verify that it states how often audit logs shall be reviewed by the Auditor per an AO/DAA defined time period. (DAR-AU-3)

4) Inspect the organization's implementing policy to verify how often the Auditor shall physically account for all EUDs in the DAR solution per an AO/DAA defined time period. (DAR-AU-4)

Expected Results:

For Step 1, a procedure is in place to inspect EUDs for malicious physical changes. For Step 2, all occurrences of auditable events given should generate an entry in the audit log. For Steps 3 and 4, ensure the implementing organization has a policy that complies with those requirements.

14.6 KEY MANAGEMENT

This section contains procedures to ensure that the generation and management of keys used in the DAR solution follow the requirements given in this Capability Package.

Requirements being tested: DAR-KM-2.

Procedure Description:

1) Verify that the DAR Components are initially keyed within a physical environment certified to protect the highest classification level of the DAR solution. (DAR-KM-2)

Expected Results:

All DAR Components should be keyed properly according to the requirements found in this Capability Package.

14.7 IMPLEMENTATION OF GUIDANCE

This section ensures there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the DAR solution. It also ensures the personnel are in place to manage and administer this solution following the guidelines given in the Capability Package.

Requirements being tested: DAR-GD-1 through DAR-GD-19, DAR-EU-2.

Procedure Description:

1) Verify the use and handling requirements given in DAR-GD-1 through DAR-GD-19 and DAR-EU-2 are currently in place and known to the users.

Expected Results:

For Step 1 all of these procedures have been followed or are in place.

14.8 INCIDENT REPORTING GUIDANCE

This section ensures that procedures are followed regarding incident reporting to NSA in the event a solution owner identifies a security incident which affects the solution.

Requirements being tested: DAR-RP-1 through DAR-RP-6.

Procedure Description:

1) Verify the requirements for reporting security incidents to the NSA given in DAR-RP-1 through DAR-RP-6 are currently in place and known to the users.

Expected Results:

For Step 1 all of these procedures have been followed or are in place.

APPENDIX A. GLOSSARY OF TERMS

Administration Workstation - This device is commonly used for logging, configuration review, and management of the EUD.

Assessment - The technical evaluation of a systems' security features, made as part of and in support of the approval/accreditation process that establishes the extent to which a particular computer systems design and implementation meet a set of specified security requirements.

Assessment and Authorization (A&A) - A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37).

Assurance - A measure of confidence that the security features and design of an AIS accurately mediates and enforces the security policy.

Audit - The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rouge behavior.

Authorization - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

Capability Package (CP) - The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. This package will point to potential products that can be used as part of this solution.

Committee on National Security Systems Policy No. 15 (CNSSP-15) - Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Designated Approving Authority (DAA) - The official with the authority to formally assume responsibility for opening a system at an acceptable level of risk, synonymous with designating accrediting authority and delegated accrediting authority. [CNSSI 4009]

End User Device (EUD) - A personal computer (desktop or laptop), consumer device (e.g., PDA, smart phone), or removable storage media (e.g., USB flash drive, memory card, external hard drive, writeable CD/DVD) that can store information.

Full Disk Encryption (FDE) - Also known as whole disk encryption, is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the FDE product.

Federal Information Processing Standards (FIPS) - A set of standards that describe the handling and processing of information within governmental agencies.

File Encryption (FE) - File encryption is the process of encrypting individual files or sets of files on an end user device and permitting access to the encrypted data only after proper authentication is provided.

Found Device - A lost device that has been recovered. (See Lost Device definition)

Software Full Disk Encryption (SWFDE) - A software product that provides Full Disk Encryption.

Lost Device - A device that is removed from the control of the physical security procedures defined by the AO/DAA.

Positive Control – The AO/DAA defines what is considered "Positive Control".

Pre-Boot Environment (PBE) - The initial software that is executed on start-up of the EUD which requires a user to authorize successfully before decrypting and booting an operating system. This is the layer of authentication for the SWFDE product.

Protection Profile (PP) - A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Salt - A salt is a non-secret value that is used in a cryptographic process, usually to ensure that the results of the computations for one instance cannot be reused by an attacker.

Supply Chain Risk Management (SCRM) - A program to establish processes and procedures to minimize acquisition-related risks to critical acquisitions including, hardware components and software solutions from supply chain threats due to reliance on global sources of supply.

Unauthorized State - The state an EUD is in when the identity of a user, user device, or other entity has not been verified.

Volume - a collection of separate units of logically divided media (partition) acting as a single entity that has been formatted with a file system.

APPENDIX B. ACRONYMS

Acronym	Definition
A&A	Assessment and Authorization
AES	Advanced Encryption Standard
AO	Authorizing Official
BIOS	Basic Input/Output System
C&A	Certification and Accreditation
CBC	Cipher Block Chaining
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Capability Package
CSfC	Commercial Solutions for Classified
DAA	Designated Approving Authority
DAR	Data-at-Rest
DEK	Data Encryption Key
DH	Diffie Hellman
DIT	Data in Transit
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EUD	End User Device
FE	File Encryption
FEK	File Encryption Key
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards
IA	Information Assurance
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alert

Acronym	Definition
ICT	Information and Communication Technology
ISSO	Information System Security Officer
JIMS	Joint Incident Management System
KEK	Key Encryption Key
MAC	Message Authentication Code
MDF	Mobile Device Fundamentals
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
OEM	Original Equipment Manufacturer
OPSEC	Operational Security
OS	Operating System
PBE	Pre-Boot Environment
PMO	Project Management Office
POC	Point of Contact
PP	Protection Profile
PUB	Publication
RFC	Request for Comment
RA	Risk Assessment
RAM	Random Access Memory
RSA	Rivest Shamir Adelman algorithm
S3	Secure Sharing Suite
SA	Security Administrator
SCRM	Supply Chain Risk Management
SF	SWFDE and FE
SHA	Secure Hash Algorithm
SIPRNet	Secret Internet Protocol Router Network
SW	Software
SWFDE	Software Full Disk Encryption
T&E	Test and Evaluation

Acronym	Definition
USB	Universal Serial Bus
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

APPENDIX C. CSFC INCIDENT REPORTING TEMPLATE

Point of Contact (POC) name, phone, email:	
Alternate POC name, phone, email:	
CSfC Registration Number:	
Classification level of affected system:	
Name of affected network(s):	
Affected component(s) manufacturer/vendor:	
Affected component(s) model number:	
Affected component(s) version number:	
Date and time of incident:	
Description of incident:	
Description of remediation activities:	
Is Technical Support from NSA Requested? (Yes/No)	

APPENDIX D. MAPPINGS TO NIST SP 800-53 CONTROLS

The mappings in Table 17 are formatted to align with the numbering scheme used in the NIST 800-53 document. The mappings below are correlated to CNSS Instruction No. 1253, Security Categorization and Control Selection for National Security Systems. CNSS 1253 provides a process for security categorization of National Security Systems (NSS) that collect, generate, process, store, display, transmit, or receive National Security Information. Most of the requirements in this Capability Package support the implementation of security controls specified in NIST SP 800-53 Revision 4. This appendix is provided for customers who must demonstrate implementation of a set of NIST SP 800-53 security controls as part of their C&A process for a system incorporating a DAR solution that complies with this Capability Package.

Note that the presence of a mapping between a requirement and a NIST SP 800-53 security control does not necessarily indicate that the requirement is by itself sufficient to fully address the security control. Instead, it indicates that implementation of the requirement provides some degree of support to implementation of the security control. Additional work outside the scope of this Capability Package may be needed for the overall system to implement the security control.

Table 17: Mappings to NIST SP 800-53 Security Controls

Req #	Solution Design	NIST SP 800-53 Revision 4 Security Controls
DAR-TR-1	SF	SI-2, SI-4(9), SI-6(c)
DAR-PS-1	SF	SA-4(6), SA-4(7)
DAR-PS-2	SF	SA-4(6), SA-4(7)
DAR-PS-3	SF	PL-8(2)
DAR-PS-4	SF	SA-12, SA-13, SA-4(6), SA-9(1(a))
DAR-PS-5	SF	SC-12(3), SC-13
DAR-SR-1	SF	AC-2(I), IA-5(1), IA-5(5)
DAR-SR-2	SF	CM-2, CM-6(2), CM-9
DAR-SR-3	SF	IA-2(5)
DAR-CR-1	SF	SC-12, IA-3(2), IA-4(d), IA-5(e), IA-5(h), IA-5(5)
DAR-CR-2	SF	IA-2(5)
DAR-CR-3	SF	SC-13
DAR-CR-4	SF	AU-2, AC-7(2), IA-2, IA-3(1), IA-4(4), IA-5(1), IA-6, IA-11, PL-8(1)
DAR-CR-5	SF	AU-2, IA-5(d), AC-7(2)

Req #	Solution Design	NIST SP 800-53 Revision 4 Security Controls
DAR-CR-6	SF	SC-12(2)
DAR-CR-7	SF	CM-5(5a), CM-6(d)
DAR-CR-8	SF	SC-28(1), SC-12
DAR-CR-9	SF	SC-28(1)
DAR-CR-10	SF	SA-4(5, 6, 7)
DAR-CR-11	SF	AC-1, AC-2(d), AC-3(3),
DAR-SW-1	SF	SC-13
DAR-SW-2	SF	
DAR-SW-3	SF	IA-5, IA-2
DAR-FE-1	SF	SC-13
DAR-FE-2	SF	AU-2, IA-5(d), AC-7
DAR-FE-3	SF	CM-7, AC-2, AC-6
DAR-FE-4	SF	IA-5, IA-2
DAR-EU-1	SF	PE-2(1), MA-1, MA-4, MA-2(b)
DAR-EU-2	SF	MA-3, MP-4, MP-6(8)
DAR-EU-3	SF	CM-6, SI-2, SA-13
DAR-EU-4	SF	PS-6
DAR-EU-5	SF	AT-2, AT-3, PM-13
DAR-EU-6	SF	PS-6
DAR-EU-7	SF	SC-12(3), SC-13(2)
DAR-EU-8	SF	IA-5(d, h)
DAR-EU-9	SF	AC-6(1)
DAR-EU-10	SF	CM-3
DAR-EU-11	SF	PE-2(1), MA-1, MA-4, MA-2(b), CM-5
DAR-EU-12	SF	PE-2(1), MA-1, MA-4, MA-2(b), CM-5
DAR-EU-13	SF	AC-19(4c), AT-1, IR-6, AC-1, IR-6
DAR-EU-14	SF	AC-1, AC-3(3), AC-6, AC-6(10), PL-8, SA-10, SA-13, SC-3(2), SC-28
DAR-CM-1	SF	AU-3(2), CM-2(1)
DAR-CM-2	SF	CM-3(1)
DAR-CM-3	SF	CM-3(1e)

Req #	Solution Design	NIST SP 800-53 Revision 4 Security Controls
DAR-DM-1	SF	PE-2(1), MA-1, MA-4, MA-2(b), CM-5
DAR-DM-2	SF	AC-17, AU-2, SC-7(3)
DAR-DM-3	SF	CM-2, SC-7(13), SC-7(21), SC-3(5)
DAR-DM-4	SF	CM-2, SC-7, SC-7(21), SC-8, PE-1
DAR-AU-1	SF	SA-19(4), SC-38, SA-12
DAR-AU-2	SF	AU-2, AU-3, AU-1
DAR-AU-3	SF	AU-6
DAR-AU-4	SF	AU-1, PM-5
DAR-AU-5	SF	CM-3, CM-9
DAR-KM-1	SF	SC-13
DAR-KM-2	SF	SC-12(2,3)
DAR-KM-3	SF	IA-5(2), SC-7, IA-7, AU-10
DAR-GD-1	SF	PS-7, SA-1, SA-4(5), SA-9(1a), SA-12, SA-13
DAR-GD-2	SF	SA-4(6)
DAR-GD-3	SF	SA-4(6), CA-1, CA-2(2), CA-7
DAR-GD-4	SF	SA-4(6), CA-6, CA-7
DAR-GD-5	SF	SA-4(6), CA-7
DAR-GD-6	SF	SA-4(6), CA-6, CA-7
DAR-GD-7	SF	AC-6, SA-13, SA-1, SA-4, MA-5(2), PS-3
DAR-GD-8	SF	AC-2(7), AC-5
DAR-GD-9	SF	PM-13
DAR-GD-10	SF	IA-5
DAR-GD-11	SF	AC-5, AC-6(5), CM-9(1), CM-2
DAR-GD-12	SF	SA-3, SI-2
DAR-GD-13	SF	SI-1
DAR-GD-14	SF	AC-19, CM-5(3), CM-11, IA-3
DAR-GD-15	SF	AC-1, AC-7(2), AC-16(6), SC-12, SC-13, MP-6(8), MP-7
DAR-GD-16	SF	AC-4(6), IR-9, AC-4(19)
DAR-GD-17	SF	MP-6, SI-12, SA-19(3)
DAR-GD-18	SF	AT-2, SI-12, CM-7
DAR-RP-1	SF	IR-5, IR-6

Req #	Solution Design	NIST SP 800-53 Revision 4 Security Controls
DAR-RP-2	SF	IR-6
DAR-RP-3	SF	IR-6
DAR-RP-4	SF	IR-6
DAR-RP-5	SF	IR-6
DAR-RP-6	SF	IR-5, IR-6, IR-7
DAR-TR-1	SF	SI-2, SI-4(9), SI-6(c)

APPENDIX E. PASSWORD/PASSPHRASE STRENGTH PARAMETERS

This appendix is intended to provide password and passphrase parameters for use in DAR products to address attacks directly based on the strength of the password or passphrase. It describes what factors provide strength to passwords and passphrases and sets a minimum bar for use.

Strength

Entropy is used as a measure of strength for passwords and passphrases. According to NIST SP800-63-2, Electronic Authentication Guideline, entropy is a measure of the amount of uncertainty that an attacker faces to determine the value of the secret. Entropy is usually stated in bits; for example an unpredictable password with 10 bits of entropy would have 2^{10} or 1,024 possible combinations. The greater the number of possible combinations, the greater the amount of time on average it will take an attacker to find the correct password or passphrase.

Random vs. User Generated

Passwords and passphrases can either be generated randomly or chosen by the user. A randomly generated value has the benefit that it will provide an objective amount of entropy, but can be difficult for a user to remember. A user generated value may be easier to remember, but may be predictable, therefore lowering the entropy calculation reducing the strength of the password or passphrase. There are many suggested methods for the user generation of passwords, more information on these can be found in NIST SP800-118, Guide to Enterprise Password Management. These methods attempt to reduce the predictability while maintaining length and memorability, but because they are user chosen they are all still at risk of being predicable. If the password or passphrase is predicable an attacker could try a much shorter list of common or personal values reducing the average time to find the correct password or passphrase. The most effective way to ensure the password or passphrase has an appropriate amount of entropy is by applying random generation.

Randomly Generated Passwords

The strength of a password is determined by the character set and the length. The character set describes the group of unique characters that may be chosen to create the password, such as numbers, lower case letters, upper case letters, special characters, etc. The length simply describes the number of characters chosen.

Randomly Generated Passphrases

The strength of a passphrase is determined by the number of words in the passphrase and the number of words in the word list, the pool of unique words that can be chosen for the passphrase.

The word list can be adjusted by the properties of the words it includes, such as minimum word length, maximum word length, and complexity (factors such as the difficulty of the word, capitalization, character substitutions, etc.) per word. Each property has a tradeoff between strength and usability. A minimum word length of four is recommended to maintain the effectiveness of the passphrase. This ensures the entropy per set of characters of a given word is greater than the entropy provided selection of a word from the word list.

Assumptions

The product is assumed to meet one of the DAR protection profiles. All password and passphrase conditioning assumes salting is performed, making pre-computed attacks infeasible. The product is assumed to be kept up to date and protection mechanisms used in calculations cannot be bypassed.

Minimum Strength Calculations

Table 18 and Table 19 show the required minimum length of a password and passphrase given a set of characters or words. The user must define the size of the character set or word list they will use. To use the tables find the value that is less than or equal to your character set (or word list) size in the Character Set Size (or Word List Size) column and the corresponding value in the Minimum Password Length (or Minimum Passphrase Length) column for that row reflects the minimum password (or passphrase) length that shall be used.

Table 18: Randomly Generated Minimum Password Length

Randomly Generated Passwords	
Character Set Size	**Minimum Password Length**
75	16
58	17
47	18
38	19
32	20
27	21
23	22
21	23
18	24
16	25
15	26
13	27
12	28
11	29
10	30

Table 19: Randomly Generated Minimum Passphrase Length

Randomly Generated Passphrases	
Word List Size	**Minimum Passphrase Length**
1000000	5
100000	6
20000	7
6000	8
2200	9
1000	10

User generated passwords shall use 14 character passwords or follow local policy. User generated passphrases shall follow local policy.

APPENDIX F. REFERENCES

CNSS 1253	*CNSS Instruction No. 1253, Security Categorization and Control Selection for National Security Systems*	October 2009
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems www.cnss.gov/Assets/pdf/cnssi_4009.pdf*	April 2010
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	March 2010
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
CSfC	*CSfC Incident Reporting Guidelines*	June 2014
CSfC Components List	*CSfC Components List* *available on the CSfC web page http://www.nsa.gov/ia/programs/csfc_program*	May 2014
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000)*	June 2009
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf*	March 2006
FE EP	*File Encryption Extended Package. www.niap.ccevs.org/pp*	**[in draft, update]**
MDF PP	*Mobile Device Fundamentals Protection Profile. www.niap.ccevs.org/pp*	October 2013

NSA Suite B	*NSA Guidance on Suite B Cryptography [including the Secure Sharing Suite (S3)]. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml*	November 2010
SW FDE PP	*Software Full Disk Encryption Protection Profile. www.niap.ccevs.org/pp*	February 2013
SP 800-56A	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. E. Barker, D. Johnson, and M. Smid*	March 2007
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. E. Barker, et. al.*	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion. L. Chen.*	November 2011
SP 800-63-2	*NIST Special Publication 800-63-2, Electronic Authentication Guideline*	August 2013
SP 800-111	*NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices*	November 2007
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths. E. Barker.*	January 2011
SP 800-132	*Recommendation for Password-Based Key Derivation*	December 2010
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines. D. Cooper, et. al.*	April 2011